Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996:	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information	)	
	)	
IP-Enabled Services	)	WC Docket No. 04-36
	)	

REPORT AND ORDER AND FURTHER NOTICE OF PROPOSED RULEMAKING

Adopted: March 13,2007 **Released: April 2,2007**

Comment Date: [30 days after publication in the Federal Register]
Reply Comment Date: [60 days after publication in the Federal Register]

By the Commission: Chairman Martin issuing a separate statement: Commissioners Copps and Adelstein dissenting in part and issuing separate statements: Commissioner Tate concurring in part and issuing a separate statement: Commissioner McDowell issuing a separate statement.

TABLE OF CONTENTS

I. INTRODUCTION

1. In this Order, the Commission responds to the practice of "pretexting"[1] by strengthening our rules to protect the privacy of customer proprietary network information (CPNI)[2] that is collected and held by providers of communications services (hereinafter, communications carriers or carriers).[3] Section 222 of the Communications Act requires telecommunications carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure.[4] Today, we strengthen our privacy rules by adopting additional safeguards to protect customers' CPNI against unauthorized access and disclosure.

2. Our Order is directly responsive to the actions of data brokers, or pretexters, to obtain unauthorized access to CPNI. As the Electronic Privacy Information Center (EPIC) pointed out in its

[1] As used in this Order, "pretexting" is the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records. Indeed, Congress has responded to the problem by making pretexting a criminal offense subject to fines and imprisonment. Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, 120 Stat. 3568 (2007) (codified at 18 U.S.C. § 1039).

[2] CPNI includes personally identifiable information derived from a customer's relationship with a provider of communications services. Section 222 of the Communications Act of 1934, as amended (Communications Act or Act), establishes a duty of every telecommunications carrier to protect the confidentiality of its customers' CPNI. 47 U.S.C. § 222. Section 222 was added to the Communications Act by the Telecommunications Act of 1996, Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified at 47 U.S.C. §§ 151 *et seq.*).

[3] This Order also extends the CPNI requirements to interconnected VoIP service providers. See *infra* Section IV.F. As used in this Order, the terms "communications carriers" and "carriers" refer to telecommunications carriers and providers of interconnected VoIP service.

[4] Prior to the 1996 Act, the Commission had established CPNI requirements applicable to the enhanced services operations of AT&T, the Bell Operating Companies (BOCs), and GTE, and the customer premises equipment (CPE) operations of AT&T and the BOCs, in the Computer II, Computer III, GTE Open Network Architecture (ONA), and BOC CPE Relief proceedings. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Implementation of Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, CC Docket Nos. 96-115 and 96-149, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8068-70, para. 7 (1998) (*CPNI Order*) (describing the Commission's privacy protections for confidential customer information in place prior to the 1996 Act).

petition that led to this rulemaking proceeding,[5] numerous websites advertise the sale of personal telephone records for a price. These data brokers have been able to obtain private and personal information. including what calls were made to and/or from a particular telephone number and the duration of such calls, In many cases. the data brokers claim to be able to provide this information within fairly quick time frames. ranging from a few hours to a few days. The additional privacy safeguards we adopt today will sharply limit pretexters' ability IO obtain unauthorized access to this type of personal customer information from carriers we regulate. We also adopt a Further Notice of Pi-oposed Rulemaking seeking comment on what steps the Commission should take. if any. to secure further the privacy of customer information.

11. EXECUTIVE SUMMARY

3. As discussed below. we take the following actions to secure CPNI:

- Carrier Authentication Requirements. We prohibit carriers from releasing call detail information to customers during customer-initiated telephone contact except when the customer provides a password. If a customer does not provide a password. we prohibit the release of call detail information except by sending it to an address of record or by the carrier calling the customer at the telephone of record. We also require carriers to provide mandatory password protection for online account access. Howevei-. we permit carriers to provide CPNl to customers based on in-store contact with a valid photo ID.

- Notice to Customer of Account Changes. We require carriers to notify the customer immediately when a password. customer response to a back-up means of authentication for lost or forgotten passwords. online account. or address of record is created or changed.

- Notice of Unauthorized Disclosure of CPNI. We establish a notification process for both law enforcement and customers in the event of a CPNI breach.

- Joint Venture and Independent Contractor Use of CPNl. We modify our rules to require carriers to obtain opt-in consent from a customer before disclosing a customer's CPNl to a carrier's joint venture partners or independent contractors for the purposes of marketing communications-related services IO that customer.

- Annual CPNI Certification. We amend the Commission's rules and require carriers to file with the Commission an annual certification, including an explanation of any actions taken against data brokers and a summary of all consumer complaints received in the previous year regarding the unauthorized release of CPNl.

- CPNI Regulations Applicable to Providers of Interconnected VoIP Service. We extend the application of the CPNl rules to providers of interconnected VoIP service.

- Enforcement Proceedings. We require carriers to take reasonable measures to discover and protect against pretexting. and, in enforcement proceedings. will infer from evidence of unauthorized disclosures of CPNl that reasonable precautions were not taken.

[5] Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information. CC Docket No. 96-115 (filed Aug. 30. 2005) (EPIC Petition).

- **Business Customers.** In limited circumstances. we permit carriers to bind themselves contractually to authentication regimes other than those adopted in this Order for services they pi-ovide to their business customers that have a dedicated account representative and contracts that specifically address the carrier's protection of CPNl.

111. BACKGROUND

A. Sertion 222 and the Commission's CPNl Rules

4. *Statutory Authority.* In section *222.* Congress created a framework to govern telecommunications carriers' protection and use of information obtained by virtue of providing a telecommunications service.[6] The section *222* framework calibrates the protection of such information from disclosure based on the sensitivity of the information. Thus. section 222 places fewer restrictions on the dissemination of information that is not highly sensitive and on information the customer authorizes to be released. than on the dissemination of more sensitive information the carrier has gathered about particular customers.[7] Congress accorded CPNI. the category of customer information at issue in this Order. the greatest level of protection under this framework.

---

[6] Section 222(a) imposes a general duly on telecommunications carriers to protect the confidentiality of proprietary information – a duty owed to other carriers. equipment manufacturers. and customers. 47 U.S.C. § 222(a). Section 222(b) states that a carrier that receives or obtains proprietary information from other carriers in order to provide a telecommunications service may only use such information for that purpose and may not use that information for its own marketing efforts. 47 U.S.C. § 222(b). Section 222(c) outlines the confidentiality protections applicable to customer information. 47 U.S.C. § 222(c). Section 222(d) delineates certain exceptions to the general principle of confidentiality. 47 U.S.C. § 222(d). The Commission addressed the scope of section 222(e) in the ***Subscriber Lisr*** *Information Order* and ***Order on Reconsider-arion.*** *Implementation ofrhe Telecommunications Arr of 1996: Telecommunications Carriers' Use* of *Customer Proprietary Network Information and Other Cusromer Information. Implementation* of *rhe Local Competition Provisions* of *the Telecommunications Acr of 1996. Provision of Direcron Lisring Information Under rhe Telecommunications Act of 1934. as amended.* CC Docket Nos. 96-115. 96-98. and 99-273. Third Report and Order, Second Order on Reconsideration. and Notice of Proposed Rulemaking. 14 FCC Rcd 15550 (1999) ***(Subscriber Lisr*** *Information Order). on reconsideration.* CC Docket No. 96-115. Memorandum Opinion and Order on Reconsideration, 19 FCC Rcd 18439 (2004) ***(Order on*** *Reconsideration*).

[7] The Commission's previous orders in this proceeding have addressed three general categories of customer information to which different privacy protections and carrier obligations apply pursuant to section 222: (I) individually identifiable CPNI. (2) aggregate customer information. and (3) subscriber list information. ***See. e.g.***, ***CPNl Order.*** 13 FCC Rcd 8061; *Implementation of rhe Telecommunications Act of* 1996: *Telecommunications Carriers' Use* of *Cusromer Proprieran Network Information and Orher Customer Information. Implementation* of *rhe Local Competition Provisions of the Telecommunications Acr* of *1996. Provision* of *Directory Listing Information Under the Telecommunications Acr of 1934. as amended.* CC Docket Nos. 96-115. 96-98. and 99-273. Order on Reconsideration and Petitions for Forbearance. 14 FCC Rcd 14409 (1999) ***(CPNI Reconsideration Order):Implementation*** of ***rhe*** *Telecommunications Acr of* 1996: *Telecommunications Carriers' Use* of *Customer Pi-oprieran Network Information aid Orher Cusromer Information. Implementation of rhe Local Comperirion Provisions of the Telecommunications Act of 1996. Provision of Directory Lisring Information Under rhe Telecommunications Acr of 1934. as amended.* CC Docket Nos. 96-115. 96-98. and 99-273. Clarification Order and Second Further Notice of Proposed Rulemaking. 16 FCC Rcd 16506 (2001): *Implementation of the Telecommunications Arr of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information arid Other Customer Information and Implementation of Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934. as amended: 2000 Biennial Regulatory Review – Review of Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers.* Third Report and Order and Third Further Notice of Proposed Rulemaking. CC Docket Nos. 96-115. 96-149. and 00-257. 17 FCC Rcd 14860 (2002) (*Third Report and Order*).

5. CPNI is defined as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by vinue of the carrier-customer relationship: and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."[8] Practically speaking, CPNI includes information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting. CPNI therefore includes some highly-sensitive personal information.

6. Section *222* reflects the balance Congress sought to achieve between giving each customer ready access to his or her own CPNI, and protecting customers from unauthorized use or disclosure of CPNI. Every telecommunications carrier has a general duty pursuant to section 222(a) to protect the confidentiality of CPNI.[9] In addition, section 222(c)(1) provides that a carrier may only use, disclose, or permit access to customers' CPNI in limited circumstances: (1) as required by law;[10] (2) with the customer's approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service." Section *222* also guarantees that customers have a right to obtain access to, and compel disclosure of, their own CPNI.[12] Specifically, pursuant to section 222(c)(2), every telecommunications carrier must disclose CPNI "upon affirmative written request by the customer, to any person designated by the customer."[13]

7. *Existing Safeguards.* On February *26,* 1998, the Commission released the ***CPNI Order*** in which it adopted a set of rules implementing section 222.[14] The Commission's CPNI rules have been amended from time to time since the ***CPNI Order,*** primarily in respects that do not directly impact the issues raised in this Order. Hence, we focus on the substance of the Commission's rules most relevant to this Order, and briefly review the history of the creation of those rules only to the extent necessary to provide appropriate context for the actions we take today."

8. In the ***CPNI Order*** and subsequent orders, the Commission promulgated rules implementing the express statutory obligations of section ***222.*** Included among the Commission's CPNI regulations implementing the express statutory obligations of section *222* are requirements outlining the extent to which section 222 permits carriers to use CPNI to render the telecommunications service from which the

---

[8] 47 U.S.C. § 222(h)(1).

[9] 47 U.S.C. § 222(a)

[10] *See, e.g., Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,* CC Docket No. 96-115, Declaratory Ruling, 21 FCC Rcd 9990 (2006) (clarifying that section *222* does not prevent a telecommunications carrier from complying with the obligation in 42 U.S.C. § 13032 to report violations of specific federal statutes relating to child pornography).

[11] 47 U.S.C. § 222(c)(1). Subsequent to the adoption of section 222(c)(1), Congress added section 222(f). Section 222(f) provides that for purposes of section 222(c)(1), without the "express prior authorization" of the customer, a customer shall not be considered to have approved the use or disclosure of or access to (1) call location information concerning the user of a commercial mobile service or (2) automatic crash notification information of any person other than for use in the operation of an automatic crash notification system. 47 U.S.C. § 222(f).

[12] *See CPNI Order,* 13 FCC Rcd at 8101-02, para. 51.

[13] 47 U.S.C. § 222(c)(2)

[14] *See CPNI Order,* 13 FCC Rcd 8061

[15] The Commission summarized the history of the CPNI proceeding in the *Third Report and Order. See Third Report and Order,* 17 FCC Rcd at 14863-72, paras. 5-25

CPNI was derived."[16] Beyond such use, the Commission's rules require carriers to obtain a customer's knowing consent before using or disclosing CPNI. As most relevant to this Order, under the Commission's existing rules, telecommunications carriers must receive opt-out consent before disclosing CPNI to joint venture partners and independent contractors for the purposes of marketing communications-related services to customers.[17] Consistent with section 222(c)(2), the Commission's rules recognize that a carrier must comply with the express desire of a customer seeking the disclosure of his or her CPNI.[18]

9. In addition to adopting restrictions on the use and disclosure of CPNI, the Commission in the *CPNI Order* also adopted a set of rules designed to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI.[19] Among these safeguards are rules that require carriers to design their customer service records in such a way that the status of a customer's CPNI approval can be clearly established."[20] The Commission also requires telecommunications carriers to train their personnel as to when they are and are not authorized to use CPNI, and requires carriers to have an express disciplinary process in place."[21] The Commission's safeguard rules also require carriers to maintain records that track access to customer CPNI records. Specifically, section 64.2009(c) of the Commission's rules requires carriers to "maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI," and to maintain such record? for a period of at least one year.[22] The Commission's safeguard rules also require the establishment of a supervisory review process for outbound marketing

---

[16] As the Commission discussed in the *CPNI Ordrr-*, "the language of section 222(c)(1)(A) and (B) reflects Congress' judgment that customer approval for carriers to use, disclose, and permit access to CPNI can he inferred in the context of an existing customer-carrier relationship. This is so because the customer is aware that its carrier has access to CPNI, and, through subscription to the carrier's service, has implicitly approved the carrier's use of CPNI within that existing relationship." CPNI ***Order***, 13 FCC Rcd at 8080, para. 23 (introducing the "total service approach" to define the boundaries of a customer's implied consent concerning use of CPNI); see ***also*** 47 C.F.R. § 64.2005(a).

[17] 47 C.F.R. § 64.2007(b); ***but see infra*** Section IV.D. (modifying this disclosure requirement to require customer opt-in consent). A customer is deemed to have provided "opt-out approval" if that customer has been given appropriate notification of the carrier's request for consent consistent with the Commission's rules and the customer has failed to object to such use or disclosure within the waiting period described in section 64.2008(d)(1) of the Commission's rules, a minimum of 30 days. 47 C.F.R. § 64.2003(i); see ***also*** 47 C.F.R. § 64.2008(d)(1). Under the Commission's rules, carriers must also receive a customer's opt-out approval before intra-company use of CPNI beyond the total service approach. 47 U.S.C. § 64.2005(a), (b). Except as required by law, carriers may not disclose CPNI to third parties, or to their own affiliates that do not provide communications-related services, unless the consumer has given opt-in consent, which is express written, oral, or electronic consent. 41 C.F.R. §§ 64.2005(b), 64.2007(b)(3), 64.2008(e); see ***also*** 47 C.F.R. § 64.2003(h) (defining "opt-in approval").

[18] 47 U.S.C. § 222(c)(2); see also, *e.g.*, ***CPNI Order***, 13 FCC Rcd at 8101-02, para. 53; 47 C.F.R. § 2005(b)(3) (prohibiting the disclosure of CPNI without opt-in consent except as permitted by section 222 of the Act or the Commission's rules).

[19] ***See CPNI Order***, 13 FCC Rcd at 8195, para. 193

[20] 47 C.F.R. § 64.2009(a); *see also CPNI Order*, 13 FCC Rcd at 8198, para. 198

[21] 47 C.F.R. § 64.2009(b); *see also* CPNI *Order*, 13 FCC Rcd at 8198, para. 198

[22] 47 C.F.R. § 64.2009(c); *see also CPNI Order*, 13 FCC Rcd at 8198-99, para. 199.

campaigns.[23] Finally. the Commission requires each carrier to certify annually regarding its compliance u ith the carrier's CPNI requirements and to make this certification publicly available:[24]

B. *IP-Enabled Services Notice*

10. On March 10. 2004. the Commission initiated a proceeding to examine issues relating to Internet Protocol (IP)-enabled sei-vices – services and applications making use of IP. including. but not limited to VoIP sei-vices?' In the *IP-Enabled Notice*. the Commission sought comment on. among other things. whether to extend the CPNI requirements to any provider of VoIP or other IP-enabled services.''

C. *EPIC CPNI Notice*

11. On August 30. 2005. EPIC filed a petition ***with*** the Commission asking the Commission to investigate telecommunications can-iers' current security practices and to initiate a rulemaking proceeding to consider establishing more stringent security standards for telecommunications carriers to govern the disclosure of CPNI.[27] In particular, EPIC proposed that the Commission consider requiring the use of consumer-set passwords. creatinp audit trails. employing encryption. limiting data retention. and improving notice procedures.[28] On February 14.2006. the Commission released the ***EPIC CPNI*** Notice. in which it sought comment on (a) the nature and scope of the problem identified by EPIC. including pretexting. and (b) what additional steps. if any. the Commission should **take** to protect further the privacy of CPNI.[29] Specifically. the Commission sought comment on the five EPIC proposals listed above. In addition. the Commission tentatively concluded that it should amend its rules lo require carriers annually to file their section 64.2009(e) cenifications with the Commission.'' It also sought comment on whether it should require carriers to obtain a customer's opt-in consent before the carrier shares CPNI with its joint venture partners and independent contractors: whether to impose rules relating to how carriers verify customers' identities: whether to adopt a set of security requirements that could be used as the basis for liability if a carrier failed to implement such requirements. or adopt a set of security requirements that a carrier could implement to exempt itself from liability: whether VoIP service providers or other IP-enabled service providers should he covered by any new rules the Commission adopts in the present rulemaking; and other specific proposals that might increase the protection of CPNI.

---

[23] 47 C.F.R. § 64.2009(d); ***see also CPNI Order.*** 13 FCC Rcd at **8199.** para. 200

[24] 47 C.F.R. § 64.2009(e); ***see also CPNI Reconsideration Order.*** 14 FCC Rcd at 14468 n.331 (clarifying that carriers must "make these certifications available for public inspection. copying and/or printing at any time during regular business hours at a centrally located business office of the carrier"). The Commission's rules also require carriers to notify the Commission in writing within five business days of any instance in which the opt-out mechanisms did not work properly. to such a degree that consumers' inability to opt-out is more than an anomaly. 47 C.F.R. § 64.2009(f); ***see Third Report and Or-der.*** 17 FCC Rcd at 14910-11. paras. 114-15 (adopting such requirement).

[25] ***See If-Embled Services.*** WC Docket No. 04-36. Notice of Proposed Rulemaking. 19 FCC Rcd 4863 (2004) (***IP-Enabled Services Norice).***

[26] ***IP-Enabled Services Notice***. 19 FCC Rcd at 4910. para. 71

[27] *See* EPIC Petition

[28] ***See id.***

[29] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information: Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*. CC Docket No. 96-115. Notice of Proposed Rulemaking. 21 FCC Rcd 1782 (2006) (*EPIC CPNI Notice or Notice*).

[30] *See id.* at 1793. para. 29

IV. DISCUSSION

12. In this Ordei-. we adopt necessary pi-otections put forward by EPIC to ensure the privacy of CPNI. The carriers' record on protecting CPNl demonstrates that the Commission must take additional steps to protect customers from carriers that have failed to adequately protect CPNI." The Attorneys General of dozens of states cite numerous suits by telecommunications carriers seeking IO enjoin pretexting activities – a clear indication that pretexters have been successful at gaining unauthorized access to CPNI." Cingular.[33] Sprint.[34] T-Mobile." Verizon Wireless[36] and other companies have sued

[31] For example. the Enforcement Bureau issued Notices of Apparent Liability against Cheyond Communications. LLC. Alltel Corporation. and AT&T for each failing to certify that they had established operating procedures adequate to ensure compliance with the Commission's rules governing the protection and use of CPNI. ***Cbeyond Communications. LLC.*** Notice of Apparent Liability for Forfeiture. 21 FCC Rcd 4316 (2006): ***Alltel Corporation.*** Notice of Apparent Liability far Forfeiture. 21 FCC Rcd 746 (2006): ***AT&T. Inc.***. Notice of Apparent Liability for Forfeiture. 21 FCC Rcd 751 (2006). Additionally. AT&T recently notified the Commission that it failed to send its CPNl "opt-out" notice to 1.2 million customers resulting in the marketing to customers who may have otherwise opted out. *See* Letter from Davida M. Grant. Senior Counsel. AT&T Inc.. to Marlene H. Dortch. Secretary. FCC. CC Docket No. 96-115 (filed Nov. 3. 2006) (AT&T CPNl Notification). Recent investigations by law enforcement authorities. including the Chicago Police Depanment and Federal Bureau of Investigation (FBI). have documented the ease with whish a part). without proper authorization. may obtain the confidential calling records of consumers. See Law Enforcement and Phone Privacy Protection Act of 2006. H.R. Rep. No. 109-395. 109th Cong. 2d Sess. 2 (2006) (citing Frank Main. *Anyone Can **Buy Cell** Phone Records: Online **Services Raise** Security Concerns for Law Enforcement*. Chi. Sun-Times. January 5. 2006. at A3). For instance. a Chicago police official obtained call records of an undercover narcotics officer's telephone number. and received accurate call records within four hours of the request. *See* Prevention of Fraudulent Access to Phone Records Act. H.R. Rep. No. 109-398. 109th Cong. 2d Sess. 2 (2006): Frank Main. *Anyone Can Buy Cell Phone **Records**: Online Services Raise Security Concerns for Law Enforcement*. Chi. Sun Times. Jan. 5. *2006.* at A3. In 1999. law enforcement authorities discovered that an information broker sold a Los Angeles detective's pager number to an Israeli mafia memher who was trying to determine the identity of the detective's confidential information. See Frank Main. ***Cell Call Lists Reveal Your Location: Anybody Can Pay to Track Where You Used Phone.*** Chi. Sun Times. Jan. 19. 2006. at A3. Citizens themselves have also testified to the ease with which a pretexter can navigate easily around the carriers' authentication systems. For example. a political Internet blogger purchased the cell phone records of former presidential candidate General Wesley Clark. See Frank Main. ***Blogger Buys Presidential Candidare's Call List: "Nobody's Records Are Untouchable." as $90 Purchase Online Shows.*** Chi. Sun-Times. January 13, 2006, at A10. Journalist Christopher Byron also testified before Congress about his own battle with pretexters. stating that pretexters repeatedly called AT&T pretending to he him or his wife and asking for his phone records. which the pretexter was able to obtain. ***See Internet Dara Brokers and Pi-elexring: Who Has Access to Your Private Records?: Hearings Before rhe Subcommittee on Oversight and Investigations of rhe H. Comm. on Energy and Commerce,*** 109th Cong. (Sept. 29,2006) (testimony of Christopher Byron).

[32] *See* Attorneys General Comments at 3 (identifying multiple filed lawsuits). All comments and reply comments cited in this Order refer to comments and reply comments cited in CC Docket No. 96-115 unless otherwise stated.

[33] ***See. e.g.. Cingular Wireless LLC v. Data Find Solutions. Inc.: James Kesrer: 1st Source Informarion Specialists Inc.: Kenneth W. Gorman: Steven Schwartz: John Does 1-100: and XYZ Corps. 1-100.*** Case No. 1:05-CV-3269-CC (N.D. Ga. filed Dec. 23.2005): *Cingular **Wireless LLC** v. **Efindoutthetruth.com. Inc.: Lisa Loftus: Tiffany Wey: North American Services. LLC d/b/a North American Information: Tom Doyle: John Does 1-100: and XYZ Corps. 1-100***. Case No. 1:05-CV-3268-ODE (N.D. Ga. filed Dec. 23. 2005); *Cingular **Wireless LLC** v. **Global Information Group. Inc.: GIG Liquidation. Inc. f/k/a Global Information Group: Bureau of Heirs. Inc.: Edward Herzog: Laurie Misner: Robin Goodwin: John Does 1-100: arid XYZ Corps. 1-100.*** Case No. 1:06-CV-0413-TWT (N.D. Ga. filed Feb. 23. 2006); *Cingular Wireless LLC* v. *Get A **Grip** Consulting. Inc.: Paraben Corporation d/b/a Get A Grip Software Publishing: **Robert** Schroeder: **John** Does 1-100: and XYZ Corps. 1-100*. Case No. 1:06-CV-0498 (N.D. Ga. filed Mar. 2. 2006).

[34] *See. e.g.. Sprint Nextel Corp. d/b/a Sprint Nextel v. 1" Source Information Specialists. Inc., et al.*, Case No. 06001083 (02) (Broward County. Florida Cir. Ct. filed Jan. 26. 2006): *Sprint Nextel Corp. d/b/a Sprint Nextel v. All Star Investigations. Inc., et al.*, Case No. 06 01736 (Miami-Dade County. Florida Cir. Ct. filed Jan. 27.

(continued....)

dozens of people whom ~l i eacc'use of fraudulently obtaining phone records." In one of the cases filed by Cingular. Cingular states in a court-filed affidavit that certain defendants or their agents posed as an employee/agent of Cingular and as a customer of the carrier to induce Cingular's customer sei-vice representative to pi-ovide them with the call records of a targeted customer.[38] The Federal Ti-ade Commission has also filed suits against several pretexters under laws barring unfair and deceptive

(...continued from previous page)
2006): *Sprint Nextel Corp. d/b/a Sprint Nextel v. San Marco & Associates Private Investigation. Inc.. et al.*. Case No. 8:06-CV-00484-T-17TGW (MD. Fla. tiled March 17.2006).

[35] *See. e.g., 7-Mobile USA. Inc. v. C.F. Anderson et al.*. Cause No. 06-2-04163 (King County Super. Ct. Feb. 2. 2006) (Stipulated Order and Permanent Injunction): *T-Mobile USA. Inc. v. 1st Source Information Services. et al.*. Case No. 06-2-03113-0 SE.4 (King County Super. Ct. May 22. 2006) (Final Order and Judgment): *7-Mobile USA. Inc. v. AccuSearch. et al.*. Case No. 06-2-06933-1 SEA (King County Super. Ct. tiled May 18. 2006) (Stipulated Order of Injunction).

[36] *Sur. e.g., Cellco Partnership d/b/a Verizon Wireless v. Source Resources.* Permanent Injunction on Consent. Docket No. SOM-L-1013-05 (Sup.Ct. of N.J.: Law Div.: Somerset County Sept. 13. *2005):Cellco Partnership d/b/a Verizon Wireless v. Global Information Group. Inc.*. et *al.*. Order. No. 05-09757 (Fla. Cir. Ct.. 13th Judicial Circuit. Hillsborough County. Nov. 2. 2005): *Cellco Partnership d/b/a Verizon Wireless v. Data Find Solutions. Inc., et al.*. Order. No. 06-CV-326 (SRC) (D.N.J.. Jan. 31. 2006).

[37] See Matt Richtel and Miguel Helft. *An Industry Is Based on a Simple Masquerade.* N.Y. Times. Sept. 11. 2006. at C1; see *also* Charles Toutant. *Verizon Wireless Suing 'Pretexters' Who Gain Access to Customer Data.* 186 N.J.L.J. 976 *(2006)*:Marguerite E. Patrick. *Lessons Learned: Issues Exposed in the Aftermath of the Hewlett-Packard Debacle.* I Privacy & Data Protection Leg. Rep. 1 (October 2006): *Internet Data Brokers and Pretexting: Who Has Access io Your Private Records?: Hearings Before the Subcommittee on Oversight and Investigations of the H. Comm.* on *Energy and Commerce.* 109th Cong. (Sept. 26. 2006) (testimony of Michael Holden).

[38] *See* H.R. Rep. 109-398 at 2.

practices.[39] Additionally, numerous stales. including California.[40] Florida.[41] Illinois.[42] Missouri.[43] and Texas[44] have all sued data hi-okers for pretexting phone records.

A. Carrier Authentication Requirements

1. Customer-Initiated Telephone Account Access

13. We find that the release of call detail[45] over the telephone presents an immediate risk to pi-ivacy and therefore we prohibit carriers from releasing call detail information based on customer-initiated telephone contact except under three circumstances.[46] First. a carrier can release call detail

[39] *Sre Internet Data Brokers and Pretexting: Who Has Access io Your Private Records?: Hearings Before the Subcommittee on Oversight and Investigations of the H. Comm. on Energy and Commerce*. 109th Cong. I (Sept. 29. 2006) (testimony of the Joel Winston. Federal Trade Commission) (citing *FTC v. Info Search. Inc.*. No. 1:06-CV-01099-AMD (D. Md. filed May I. 2006): *FTC v. Accusearch. Inc. d/b/a Abika.com*. No. 06-CV-0105 (D. Wyo. filed May 1. 2006): *FTC v. CEO Group. Inc. d/b/a Check Em Out*. No. 06-60602 (S.D. Fla. filed May I. 2006): *FTC v. 77 Investigations. Inc.*. No. EDCV06-0439 VAP (C.D. Cal. filed May 1. 2006): *FTC v. Integrity Sec. & Investigation Servs.. Inc.*. No. 2:06-CV-241-RGD-JEB (E.D. Va. filed May 1.2006)).

[40] *See. e.g.. California v. Dain Trace USA Inc.*. No. GIC862672 (Cal. Super. Ct. filed Mar. 14. 2006)

[41] *See. e.g.. Florida v. 1" Source Information Specialists. Inc.*. No. 37-2006-CA-00234 (Fla. Cir. Ct. filed Jan. 24. 2006): *Florida v. Global Information Group. Inc.. et al.*. No. 06-1570 (Fla. Cir. Ct. filed Feb. 24. 2006).

[42] *See. e.g.. Illinois v. 1" Source Information Specialists. et al.*. No. 2006-CH-29 (Ill. Cir. Ct. filed Jan. 20. 2006): *see also* Press Release. *Office of the Attorney General. Madigan Sues Second Company that Sells Cell Phone Records* (Mar. 15. 2006). *available at* www.ag.state.il.us/pressroom/2006_03/20060315c.html (announcing ihe filing of a law suit against a Florida company that allegedly ohtsined and sold phone record5 without customer consent).

[43] See. *e.g.. Missouri v. Data Trace USA. Inc.. et a.*. No. 06AC-CC-00158 (Mo. Cir. Ct. filed Mar. 3. 2006: *see also* Press Release. Missouri Attorney General's Office. *Locatecell.com must stop selling cell phone records of Missourians. under court order obrained by Nixon* (Feb. 15.2006). *available ar* www.ago.mo.gov/newsreleases/2006/021506.htm (announcing the issuance of a court order to stop the sale of Missourians' cell phone records by several people currently or formerly associated with the website Locatecell.com).

[44] *See. e.g., Texas v. John Strange d/b/a USA Skiptrace.com.* No. 06-1666 (Tex. Dist. Ct. Travis County filed Feb. 9. 2006); *see also* Press Release; Attorney General of Texas. *Attorney General Abborr Files First Suit Against Sellers of Private Phone Records* (Feb. 9, 2006). *available at* http://www.oag.state.tx.us/oagnews/release.php?id=1449.

[45] "Call detail" or "call records" includes any information that pertains to the transmission of specific telephone calls including. for outbound calls. the number called. and the time. location. or duration of any call and. for inbound calls. the number from which the call was placed. and the time. location. or duration of any call. *See. e.g.. Third Report and Order.* 17 FCC Rcd at 14864. para. 7. Remaining minutes of use is an example of CPNI that is not call detail information. We disagree with commenters that argue we should adopt a more narrow definition of call detail: a narrower definition that included only inbound or outbound telephone numbers would make it too easy for unauthorized persons with partial information to confirm and expand on that information. *See. e.g.*. Letter from Jim Halpert. Counsel to the Anti-Pretexting Working Group. DLA Piper. to Marlene H. Dortch. Secretary. FCC. CC Docket No. 96-115 Attach. at 2 (filed Oct. 31.2006): Letter from William F. Maher, Jr. .Counsel for T-Mobile USA. Inc.. to Marlene H. Dortch. Secretary, FCC. CC Docket No. 96-115 at I (filed Nov. 30. 2006); Letter from Charon Phillips. Verizon Wireless. to Marlene H. Dortch. Secretary. FCC. CC Docket No. 96-115 at I (filed Dec. 1. 2006).

[46] *Spy. e.g.*. Letter lorm Donna Epps. Vice President Federal Regulatory. Verizon. to Marlene H. Dortch. Secretary. FCC. CC Docket No. 96-115 (filed Nov. 20. 2006) (arguing that any password requirement should only apply to accessing call detail information). By limiting our rules io ihe disclosure of call detail information. we believe that we have narrowly tailored our requirements to address the problem of pretexting. *See. e.g.*. AT&T Reply at 2 (arguing that the Commission should ensure that any measures taken are "narrowly tailored to address a demonstrated problem"); Letter from Donna Epps. Vice President. Federal Regulatory. Verizon. to Marlene H.

(continued....)

information if the customer provides the carrier with a pre-established password.[47] Second, a carrier may, at the customer's request, send call detail information to the customer's address of record.[48] Third, a carrier may call the telephone number of record and disclose call detail information.[49] A carrier may disclose non-call detail CPNI to a customer after the carrier authenticates the customer.[50]

14. The record reflects that pretexters use evolving methods to trick employees at customer service call centers into releasing call detail information.[51] This release of call detail through customer-initiated telephone contact presents heightened privacy concerns because of pretexters' abilities to circumvent carrier authentication requirements and gain immediate access to call detail.[52] By restricting

(...continued from previous page)
Dortch, Secretary, FCC, CC Docket No. 96-115 at Attach. (filed Jan. 29, 2007) (Verizon Jan. 29, 2007 *Ex Parte Letter*) (stating that password protecting call detail records "is a narrowly tailored solution" that "directly targets the means and methods used by pretexters"). We also limit the requirements we impose in this section to customer-initiated contact with the carrier. We find that there is not the same need for authentication when the carrier initiates contact with a customer via the telephone number of record or via the address of record. By "telephone number of record," we mean the telephone number associated with the underlying service, rather than some other telephone number supplied as a customer's "contact information." By "address of record," whether postal or electronic, we mean an address that the carrier has associated with the customer's account for at least 30 days. Requiring that the address be on file for 30 days will foreclose a pretexter's ability to change an address of record for the purpose of being sent call detail information immediately.

[47] We understand that many consumers may not like passwords and thus we only extend the use of password protection of call detail information during customer-initiated telephone calls. *See, e.g.*, AT&T Comments at 8-11 (noting studies that demonstrate customers are opposed to mandatory passwords); Centennial Comments at 3-4 (arguing that customers find passwords burdensome). Further, for those customers not interested in password protection, we provide other alternatives for carrier disclosure of call detail information that directly advance our goal of protecting against pretexter activity and will not unduly burden carrier-customer relations.

[48] This exception to the disclosure of call detail information in no way alters a carrier's usual practice of sending monthly billing statements to the customer.

[49] *See supra* note 46 (defining "telephone number of record"). We find that it is necessary for the carrier to call the customer at the telephone number of record, rather than rely on caller ID as an authentication method, because pretexters can easily replicate caller ID numbers. *See, e.g.*, Alltel Comments at 5.

[50] Although we do not enact password protection for non-call detail CPNI in this Order, carriers are still subject to section 222's duties to protect CPNI, and thus a carrier must authenticate a customer prior to disclosing non-call detail CPNI. See 47 U.S.C. § 222; *see also* Verizon Wireless Comments at 9 (arguing that "passcodes" can lead to a frustrating experience for customers seeking answers to simple billing questions). We rely on carriers to determine the authentication method for the release of non-call detail CPNI that is appropriate for the information sought and which adheres to section 222's duty. However, we seek comment on whether the Commission should impose password protection on non-call detail CPNI in today's Further Notice. *See infra* Section V.A.

[51] See, *e.g.*, Alltel Comments at 5; Cingular Comments at 13; Dobson Comments at 2; Sprint Nextel Comments at 4-5; see *also* Testimony of James Rapp, House Energy and Commerce Committee, Subcommittee on Oversight and Investigations Hearing: "Internet Data Brokers and Pretexting: Who Has Access to Your Private Records?" Attach. A (June 21, 2006) (setting forth an outline of a training manual on how to obtain call detail and other personal information), *available at* http://energ.ycommerce.house.gov/108/Hearings/06212006hearing1916/Rapp.pdf; Brad Stone, *A 'Pretexter' and His Tricks: Phone Records Are a Snap to Snag. Just Ask David Gandal*, NEWSWEEK, Sept. 10, 2006, at 43 (interviewing a pretexter who explains how pretexting is accomplished); *supra* para. 12 and accompanying notes (identifying lawsuits alleging pretexting activity).

[52] Specifically, the Attorneys General state that data brokers consistently demonstrate that they can obtain almost any type of personal information, including social security numbers and mother's maiden name, which carriers currently use to authenticate a customer. *See, e.g.*, Attorneys General Comments at 15; *see also* EPIC *et al.* Comments at 12.

the ways in which carriers release call detail in response to customer-initiated telephone calls. we place at most a minimal inconvenience on carriers and consumers.."

15. *Establishment of Password Protection.* For new customers. carriers may request that the customer establish a password at the time of service initiation because the carrier can easily authenticate the customer at that time?' For existing customers to establish a password. a carrier must first authenticate the customer without the use of readily available biographical information.[55] or account information.[56] For example. a carrier could call the customer at the telephone number of record." If a carrier already has password protection in place for a customer account. a carrier does not have to reinitialize a customer password?' By permitting the carrier to determine its authentication method. the carrier has the most flexibility for designing an authentication program that can continue to evolve to fight against pi-etexting efforts.

16. *Use of Password Protection.* For accounts that ai-e password protected, a carrier cannot obtain the customer's password by asking for readily available biographical information. or account

[53] Customers requiring instant access to call detail information also have the option of accessing such data online in the protected manner described in Section IV.A.2. or by visiting a carrier's retail location with a valid photo ID as described in Section IV.A.3.

[54] ***See.*** *e.g.*. Virgin Mobile Reply at **4** (mandating thal customers select a password at the time of the service activation process). By "new customers." we include only those customers that establish service after the effective date of our rules.

[55] "Readily available biographical information" includes such things as the customer's social security number. **os** the last four digits of that number: the customer's mother's maiden name: a home address: or a date of birth. *See. e.g.*. EPIC Petition **at *8: see also*** AT&T Comments at *3* (noting that authenticating customers by relying "solely on a customer's name. address and/or phone number may he insufficient" and that the Commission could seasonably conclude "that all carriers should authenticate a customer's identity using non-public information prior to releasing CPNI"); ***id.*** at *I* (finding that authenticating the customer based on non-public information would impose "little additional cost").

[56] **See.** *e.g.*, EPIC Reply at **2.** "Account information" includes such things as account number or any component thereof. the telephone number associated with the account. or amount of last hill.

[57] A carrier could **also** use a Personal Identification Number (PIN) method to authenticate the customer. A PIN authentication method could entail a carrier supplying the customer with a randomly-generated **PIN, not** based on readily available biographical information. **os** account information. which the customer would then provide to the carrier prior to establishing a password. Carriers could supply the PIN to the customer by a carrier-originated voicemail or text message to the telephone number of record. or by sending it **to** an address **of** record so as to reasonably ensure that it is delivered to the intended party. **See. *e.g.***., Letter from William F. Maher. Jr.. Counsel for T-Mobile USA. Inc.. Morrison & Foerster. to Marlene **H.** Dortch. Secretary. FCC, CC Docket No. 96-115 **at 2** (filed Nov. **20.2006)** (providing customers with a temporary password by sending it to the customer's mobile phone number). A carrier cannot authenticate a customer by sending the customer a PIN (or any other type of carrier chosen method of authentication) to new contact information that the customer provides **at** the time **of** the customer's PIN (or other authentication) request. Carriers could also authenticate the customer by requesting that the customer present a valid photo ID at a carrier's retail location. **A** "valid photo I D is a government-issued personal identification with a photograph such **as** a current driver's license. passport. *os* comparable ID.

[58] *See. e.g.*. Sprint Nextel Reply at 7 (noting that most carriers already allow customers to choose password protection): Letter from Donna Epps. Vice President. Federal Regulatory. Verizon. to Marlene H. Dortch. Secretary. FCC. CC Docket No. 96-115 at 7 (filed *Dec.* 22. 2006) (*Verizon Dec.* 22. 2006 *Ex Parte* Letter) (noting that Verizon already permits its custoniers to password protect telephone account access).

information. to prompt the customer For his password,"; We understand. of course. that passwords can be lost or forgotten. and share commenters' concern that security measures should not unnecessarily *inconvenience customers or impair customer* set-vice systems.[60] We therefore allow carriers to create back-up customer authentication methods for lost or forgotten passwords that ai-e also not based on readily available biographical information. or account information." For example. the Attorneys General support the use of a shared secret back-up authentication procedure for lost or forgotten passwords." As further account protection. with a shared secret back-up authentication pi-oprani. the can-ier may offer the opportunity for the customer to design the shared secret question.[63] We find that limiting back-up authentication methods to those that do not include readily available biographical information. or account information. will protect customers most effectively fi-om pretexters.

17. Although we recognize that carriers and customers will he subject to a one-time burden to implement password protection if a customer is interested in paining access to call detail during a customer-initiated telephone call. we believe that the ongoing burdens of these authentication requirements will be minimal. Further. this method balances consumers' interests in ready access to their call detail. and carriers' interests in providing efficient customer service. with the public interest in maintaining the security and confidentiality of call detail information.

18. *Alternative Access to Call Detail Information.* If a customer does not want to establish a password, the customer may still access call detail information. based on a customer-initiated telephone call. by asking the carrier to send the call detail information to an address of record or by the carrier calling the telephone number of record.[64] Because we provide multiple methods for the customer lo access call detail based on a customer-initiated telephone call. neither customers who dislike passwords

[59] We agree with commenters that assert that individuals lend to choose passwords that are based on personal information and therefore pretexters can easily circumvent password protections. *See, e.g.*. Verizon Wireless Comments at 9: Sprint Nextel Reply at 8. To prevent this. we prohibit carriers from using prompts to request the customer's password based on readily available biographical information. or account information. If a customer cannot provide the correct password and the carrier does not offer a back-up authentication method lo access call detail. the carrier must reauthenticate the customer. A carrier cannot disclose call detail information over the telephone during a customer-initiated telephone call until the carrier is able to reauthenticate the customer without the use of readily available biographical information. or account information.

[60] *See, e.g.*, Verizon Wireless Comments at 9.

[61] ***See.*** *e.g.*, Letter from Cynthia R. *Southworth*. Director of the Safety Net Project. National Network to End Domestic Violence. to Marlene H. Dortch. Secretary, FCC. CC Docket No. 96-115 at 2 (filed Nov. 30, 2006) (NNEDV Nov. 30.2006 ***Ex Pane*** Letter). We do not require carriers to adopt a specific back-up authentication method because we believe that by directing carriers to do so we might make it easier for pretexters to defeat the protections we adopt in this Order. ***See. e.g.***, Verizon Wireless Reply at 9. If a customer cannot provide the correct response to the back-up authentication method to access call detail. the carrier must reauthenticate the customer. A carrier cannot disclose call detail information over the telephone during a customer-initiated telephone call until the carrier is able to reauthenticate the customer without the use of readily available biographical information. or account information.

[62] ***See*** Attorneys General Comments at 16: *see also* Ohio PUC Comments at 9-10. A shared secret is one or more question-answer combinations that are known to the customer and the carrier but are not widely known. Thus. if the customer lost or forgot a password. the carrier could provide the pre-selected shared secret question. or set of shared secret questions. to the customer for authentication purposes.

[63] *See, e.g.*, Virgin Mobile Reply at 5 n.3 (allowing the customer to create their own back-up authentication question).

[64] The customer may also access call detail information by establishing an online account or by visiting a carrier's retail location. *See infra* Sections IV.A.2 and IV.A.3.

nor carriers concerned about timely customer service should find our requirements burdensome.[65] Furthermore. by providing a variety of secure means for customers to receive call detail information from carriers. and focusing on one of the most pi-oblematic means of pretexting – obtaining call detail information from customer service representatives without proper identity screening – our rules are no more extensive than necessary to protect consumers' privacy with respect to telephone access to account information.[66]

19. We do not intend for the prohibition on the release of call detail over the telephone for customer-initiated telephone contact to hinder routine carrier-customer relations regarding service/billing disputes and questions.[67] If a customer is able to provide to the carrier. during a customer-initiated telephone call. all of the call detail information necessary to address a customer service issue (*i.e.*, the telephone number called. when it was called. and. if applicable. the amount charged for the call). then the carrier is permitted to proceed with its routine customer care procedures."[68] We believe that if a customer is able to provide this information to the carrier. without carrier assistance. then the can-ier does not violate our rules if it takes routine customer service actions related to such information. We additionally clarify that under these circumstances. carriers may not disclose to the customer any call detail information about the customer account other than the call detail information that the customer provides without the customer first providing a password. Our rule is intended to prevent pretexter phishing and other pretexter methods for gaining unauthorized access to customer account information.

[65] *See, e.g.*, BellSouth Comments at 16 (noting the use of an optional customer-provided password for the release of CPNI over the telephone).

[66] See Verizon Dec. 22. 2006 *Ex Parte* Letter at 5 (arguing that "any password requirement would have to be narrowly crafted to address the specific problem of pretexters fraudulently obtaining call detail information").

[67] *See, e.g.*, Letter from Charon Phillips. Verizon Wireless. to Marlene H. Dortch. Secretary, FCC. CC Docket No. 96-115 at 1 (filed Dec. 1. 2006) (raising concerns about a carrier's ability to serve customers during customer service calls).

[68] *See, e.g.*, Letter from William F. Maher. Jr., Counsel for T-Mobile USA. Inc., to Marlene H. Dortch, Secretary. FCC. CC Docket No. 96-115 at 2 (filed Nov. 20.2006): Verizon Dec. 14.2006 Ex Pane Letter at 2.

2. Online Account Access

20. We also require carriers to password protect online access to CPNI.[69] Although section 222 of the Act imposes a duty on carriers to protect the privacy of CPNI.[70] data brokers and others have been able to access CPNI online without the account holder's knowledge or consent." We agree with EPIC that the apparent ease with which data brokers have been able to access CPNl online demonstrates the insufficiency of carriers' customer authentication procedures.[72] In particular, the record evidence demonstrates that some carriers permit customers to establish online accounts by providing readily available biographical information.[73] Thus. a data hi-oker may obtain online account access easily without the customer's knowledge. Therefore. we agree with EPIC and others that use of such identifiers is an insufficient mechanism for preventing data brokers from obtaining unauthorized online access to CPNI.[74]

21. To close this gap. we prohibit carriers from relying on readily available biographical information. or account information to authenticate a customer's identity before a customer accesses CPNl online. In addition. because a carrier is responsible to ensure the security and privacy of online account access. a carrier must appropriately authenticate both new and existing customers seeking access

---

[69] *See, e.g.*, Letter from John T. Scott. 111. Vice President & Deputy General Counsel Regulator!, Law. Verizon Wireless. to Marlene H. Dortch. Secretary. FCC. CC Docket No. 96-115 at 1 (filed Oct. 18. 2006) (Verizon Wireless Oct. 16 *Ex Parte* Letter) (arguing that carriers should require passwords for online access to CPNI): Verizon Dec. 22. 2006 *Ex Parte* Letter at 2 (supporting a proposal lo require password protection for customer online account access because passwords are "routine and readily accepted by customers" in the online environment). We do not limit our online account access rules to just call detail because online account access presents a heightened security risk. Specifically. online account access allows a customer (or pretexter) to *view* and *change* personal information easily (including online passwords. addresses of record. and hilling information) without carrier assistance. During a telephone conversation with the customer. a carrier is able to authenticate a customer and sense whether the customer is who he claims to he. In the online context. however. there is no person-to-person contact (or limited interactive voice recognition menu) and thus a pretexter, if he were able to circumvent online password protection. could obtain significant amounts of a customer's private informalion (including home address. plan information. billing information. and call detail records for months at a time) with only the click of a mouse. Thus. we believe that we must extend our online account access rules to include the disclosure of all CPNl to protect customer privacy. Furthermore. most carriers already require password protection for online accounts. See, *e.g.*, Verizon Dec. 22.2006 *Ex Pane* Letter at 2. They do not differentiate their online account systems between access to call detail information and non-call detail CPNI. and requiring them to do so likely would impose significant costs. For these reasons. we find that our requirements in the online context are no more extensive than necessary to protect consumers' privacy. *See Ceniral Hudson Gas & Elec. Corp. v. Public Service Comm'n of N.Y.*, 447 U.S. 557, 564-65 (1980).

[70] *See* 47 U.S.C.§ 222(a) (stating that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of. and relating to . . . customers").

[71] For instance. pretexters have been able to access CPNI by deceiving customer service representatives or by exploiting security gaps in customers' online accounts. *See. e.g.*, EPIC Petition. Appendix C (providing a list of 40 web sites offering to sell CPNl to third parties): Attorneys General Comments at 3 (describing pretexters' use of online account access).

[72] *See, e.g.*, EPIC Petition at 8. I I: *see also supra* para. 12 and accompanying notes.

[73] *See, e.g.*, EPIC Petition at 8. The record in this proceeding reveals other holes in carriers' existing authentication measures. such as authenticating a customer's identity through information the carrier readily provides to any person purporting *to* he the customer without authentication. thus enabling a prelexter to obtain online access to CPNl by first calling the carrier to obtain the information. The requirements ue adopt in this Order fix such flaws.

[74] *See, e.g.*, EPIC *et al.* Comments at 12-13 (explaining that biographical identifiers are widely available on websites and easily obtained by pretexters): Centennial Reply at 6 (stating that biographical information like social security number can be found on the Internet).

to CPNI online.[75] However, we do not require carriers to reinitialize existing passwords for online customer accounts, but a carrier cannot base online access *solely* on readily available biographical information, or account information, or prompts for such information.[76]

22. As with the password protection for the release of call detail during customer-initiated telephone contact, we understand that passwords for online access can also be lost or forgotten, and share commenters' concern that security measures should not unnecessarily inconvenience customers or impair customer service systems.[77] We therefore allow carriers to create back-up customer authentication methods for lost or forgotten passwords in line with the back-up authentication method framework established for the password protection for customer-initiated telephone contact.[78] Further, if a customer cannot provide a password or the proper response for the back-up authentication method to access an online account, the carrier must reauthenticate the customer based on the authentication methods adopted in this Order prior to the customer gaining online access to CPNI.[79] Finally, as with the establishment of the password for the release of call detail for customer-initiated telephone contact, although we recognize that carriers and customers will be subject to a one-time burden to implement this Order, we believe the ongoing burdens of these authentication requirements will be minimal and are outweighed by the benefits to consumer privacy.

3. Carrier Retail Location Account Access

23. We continue to allow carriers to provide customers with access to CPNI at a carrier's retail location if the customer presents a valid photo ID[80] and the valid photo ID matches the name on the account.[81] We agree with the Attorneys General and find that this is a secure authentication practice because it enables the carrier to make a reasonable judgment about the customer's identity.[82]

---

[75] For new customers, a carrier could request that a customer establish an online password at the time of service initiation. See ***supra*** note **54.** Alternatively, for all customers, a carrier could use a PIN method, as described above, to authenticate a customer if necessary. See ***supra*** note ***56.***

[76] Although we do not mandate what specific level of password protection carriers must provide for their customers for online access, we expect carriers to ensure that online access to CPNI is adequately password protected. For example, we believe it would be reasonable for carriers to block access to a customer's account after repeated unsuccessful attempts to log in to that account to prevent hackers from using a so-called "brute force attack" to discover account passwords. Carriers may also determine the password format they deem appropriate. For example, carriers may decide the length of the password, whether or not the password should be case-sensitive, or whether the password should require a mix of numerals, letters, and other symbols.

[77] ***See supra*** note ***60.***

[78] ***See supra*** Section IV.A.1. For existing online accounts, although we do not mandate that a carrier reinitialize those accounts, if a carrier provides a back-up authentication method that is not in conformance with this Order (*i.e.*, the method is based on carrier prompts for readily available biographical information, or account information), then a carrier must modify its back-up authentication method to comply with this Order.

[79] This requirement extends to all online accounts regardless of whether the online account access existed prior to the effective date of these rules.

[80] A "valid photo ID" is a government-issued personal identification with a photograph such as a current driver's license, passport, or comparable ID.

[81] *See, e.g.*, Cingular Comments at 18 (requiring a photo ID before providing a customer a print out of the bill at a retail location).

[82] *See* Attorneys General Comments at 16.

4. Notification of Account Changes

24. We require carriers to notify customers immediately of certain account changes. including whenever a password. customer response to a carrier-designed back-up means of authentication.[83] online account. or address of record is created or changed.[84] We agree with the New Jersey Ratepayer Advocate that this notification is an important tool for customers to monitor their account's security.[85] This notification may he through a carrier-originated voicemail or text message to the telephone number of record. or by mail to the address of record. as to reasonably ensure that the customer receives this notification.[86] We believe this measure is appropriate to protect customers from data brokers that might otherwise manage to circumvent the authentication protections we adopt in this Order. and to take appropriate action in the event of pretexter activity. Further. we find that this notification requirement will also empower customers to provide carriers with timely information about pretexting activity. which the carriers may not be able to identify easily.[87]

5. Business Customer Exemption

25. We do make on exception to the rules that we adopt today for certain business customers. We agree with commenters who ai-gue that privacy concerns of telecommunications consumers are greatest when using personal telecommunications services.[88] Indeed. the fraudulent practices described by EPIC have mainly targeted individual consumers. and the record indicates that the proprietary information of wireline and wireless business account customers already is subject to stringent safeguards, which are privately negotiated by contract.[89] Therefore. if the carrier's contract with a business customer is serviced by a dedicated account representative as the primary contact. and specifically addresses the carrier's protection of CPNI. we do not extend our carrier authentication rules to cover these business customers because businesses ai-e typically able to negotiate the appropriate

---

[83] A customer response to a carrier-designed back-up means of authentication is the customer's pre-selected answer to the carrier's back-up authentication method in the event that the customer lost or forgot his password.

[84] This notification process is not required when the customer initiates service. including the selection of a password at service initiation.

[85] *See* New Jersey Ratepayer Advocate Comments at 4: see also Alltel Comments at 5 (noting that notice of certain account changes may protect subscriber's security): Ohio PUC Comments at 10 (asserting that providing notice to customers of changed passwords is an effective strategy for protecting CPNI).

[86] *See, e.g.*, Verizon Dec. 22. 2006 *Ex* Pane Letter at 6 (arguing against a "one-size-fits-all" requirement for notifying customers of account changes on First Amendment grounds). To protect the security of the potential victim of pretexting. such notification must not reveal the changed account information. Additionally, a carrier may not notify the customer of account changes by sending notice to the new account information. which might result in the customer not being notified of the change (*e.g.*, mailing a customer's change of address to a new address rather than to the former address of record).

[87] *See, e.g.*, NCTA Comments at 6 (arguing that a carrier generally does not know when a data broker breaches carrier security measures because the carrier believes the data broker is the customer): TWTC Comments at 13 (stating that carriers usually are not aware when pretexting occurs): Cingular Reply at 7 n.17 (arguing that the customer is usually aware of a security problem before the carrier].

[88] See, *e.g.*, Letter from Donna Epps. Vice President and Federal Regulatory. Verizon. to Marlene H. Dortch. Secretary. FCC. CC Docket No. 96-115 at 2 (filed Dec. 14. 2006) (Verizon Dec. 14. 2006 *Ex Parte* Letter).

[89] *See, e.g.*, TWTC Comments at 19-20: Letter from John J. Heitmann and Jennifer M. Kashatus. Counsel to XO Communications. to Marlene Dortch. Secretary. FCC. CC Docket No. 96-115. at 2 (filed Oct. 19. 2006): Letter from Karen Reidy. Vice President. Regulatory Affairs. COMPTEL. to Marlene H. Dortch. Secretary. FCC. CC Docket No. 96-115 in 1 (filed Dec. 18. 2006) (COMPTEL Dec. 18. 2006 *Ex Parte* Letter).

protection of CPNI in their service agreements."[90] However, nothing in this Order exempts carriers serving wireline enterprise and wireless business account customers from section 222 or the remainder of the Commission's CPNI rules.

B. Notice of Unauthorized Disclosure of CPNI

26. We agree with EPIC that carriers should be required to notify a customer whenever a security breach results in that customer's CPNI being disclosed to a third party without that customer's authorization."[91] However, we also appreciate law enforcement's concern about delaying customer notification in order to allow law enforcement to investigate crimes.[92] Therefore, we adopt a rule that we believe balances a customer's need to know with law enforcement's ability to undertake an investigation of suspected criminal activity, which itself might advance the goal of consumer protection.[93]

27. In conjunction with the general rulemaking authority under the Act,[94] section 222(a), which imposes a duty on "[e]very telecommunications carrier, . . . to protect the confidentiality of proprietary information," provides ample authority for the Commission to require carriers to report CPNI breaches to law enforcement and prohibit them from disclosing breaches to their customers until after law enforcement has been notified. Notifying law enforcement of CPNI breaches is consistent with the goal of protecting CPNI. Law enforcement can investigate the breach, which could result in legal action against the perpetrators, thus ensuring that they do not continue to breach CPNI. When and if law enforcement determines how the breach occurred, moreover, it can advise the carrier and the Commission, enabling industry to take steps to prevent future breaches of that kind. Because law enforcement will be informed of all breaches, it will be better positioned than individual carriers to develop expertise about the methods and motives associated with CPNI breaches. Again, this should enable law enforcement to advise industry, the Commission, and perhaps Congress regarding additional measures that might prevent future breaches.

28. The requirement that carriers delay customer notification of breaches until after law enforcement has been notified is also consistent with these goals. Once customers have been notified, a

---

[90] These business customers are able to reach customer service representatives without going through a call center. If the business customer must go through a call center to reach a customer service representative then this exemption does not apply to that customer.

[91] See EPIC *et al.* Comments at 15; *see also, e.g.*, CaPUC Comments at 3 (recommending the adoption of a rule that carriers notify a customer when the carrier discloses a customer's CPNI without customer consent); MetroPCS Comments at 9 (stating that it notifies a customer through a text message anytime that it releases CPNI); Verizon Wireless Oct. 18.2006 *Ex Parte* Letter at 2 (arguing that customers should be aware if a carrier disclosed their data to a third party); NNEDV Nov. 30, 2006 *Ex Parte* Letter at 3 (arguing for a victim to be notified prior to law enforcement).

[92] *See* DOJ/DHS Comments at 14; Letter from Paul J. McNulty, Deputy Attorney General, United States Department of Justice, to Kevin J. Martin, Chairman, FCC, CC Docket No. 96-115 (filed Dec. 28, 2006) (DOJ Dec. 28.2006 *Ex Parte* Letter); Letter from Joseph E. Springsteen, Trial Attorney, United States Department of Justice, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 (filed Mar. 13, 2007).

[93] *See* DOJ Dec. 28, 2006 *Ex Parte* Letter; *see also* Cal. Civ. Code § 1798.82 (permitting law enforcement to delay customer notification of breaches of security if a law enforcement agency determines the notification will impede a criminal investigation); N.Y. Gen. Bus. Law § 899-aa (permitting law enforcement to delay customer notification of breaches of security if a law enforcement agency determines the notification impedes a criminal investigation).

[94] Section 201(b) authorizes the Commission to "prescribes such rules and regulations as may lie necessary in the public interest to carry out the provisions of this Act," including section 222. 47 U.S.C. § 201(b). Section 1 charges the Commission with "promoting safety of life and property through the use of wire and radio communication." 47 U.S.C. § 151.

breach may become public knowledge, thereby impeding law enforcement's ability to investigate the hi-each. identify the perpetrators, and determine how the breach occurred. In short, immediate customer notification may compromise all the benefits of requiring carriers to notify law enfoi-cement of CPNI breaches. A short delay is warranted, therefore, with the proviso that carriers may notify customers if there is an urgent need to do so to avoid immediate and irreparable harm.

29. A telecommunicalions carrier shall notify law enforcement of a breach of its customers' CPNl no later than seven business days after a reasonable determination of a breach by sending electronic notification through a central reporting facility to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI)."[95] A telecommunications carrier may notify the customer and/or disclose the hi-each publicly after seven business days following notification to the USSS and the FBI, if the USSS and the FBI have not requested that the telecommunications carrier continue to postpone disclosure.[96] A telecommunications carrier, however, may immediately notify a customer or disclose the breach publicly after consultation with the relevant investigative agency, if the carrier believes that there is an extraordinarily urgent need to notify a customer or class of customers in order to avoid immediate and irreparable harm.[97] Additionally, we require carriers to maintain a record of any discovered breaches, notifications to the USSS and the FBI regarding those breaches, as well as the USSS and the FBI response to the notifications for a period of at least two years. This record must include, if available, the date that the carrier discovered the breach, the date that the carrier notified the USSS and the FBI, a detailed description of the CPNI that was breached, and the circumstances of the breach.

30. We reject commenters' argument that the Commission need not impose new rules about notice to customers of unauthorized disclosure because competitive market conditions will protect CPNI from unauthorized disclosure.[98] If customers and law enforcement agencies are unaware of pretexting activity, unauthorized releases of CPNl will have little impact on carriers' behavior, and thus pi-ovide little incentive for carriers to prevent further unauthorized releases.[99] By mandating the notification process adopted here, we better empower consumers to make informed decisions about service providers and assist law enforcement with its investigations. This notice will also empower carriers and consumers to take whatever "next steps" are appropriate in light of the customer's particular situation."[100]

31. We clarify, however, that nothing in today's Order is intended to alter existing law regarding customer notification of law enforcement access to customer records. Therefore, for example, when

[95] The Commission will maintain a link to the reporting facility at www.fcc.gov/eb/cpni

[96] If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, the law enforcement agency may direct the carrier not to disclose the breach for an initial 30-day period. This 30-day period may be extended by the law enforcement agency as reasonably necessary in the judgment of the agency. The law enforcement agency shall provide in writing to the carrier its initial direction to the carrier and any subsequent direction.

[97] A telecommunications carrier should indicate its desire to notify its customer or class of customers immediately concurrent with its notice to the USSS and FBI of a breach.

[98] See, *e.g.*, Charter Comments at 7-9 (discussing how market forces give carriers incentive to protect CPNI); Time Warner Comments at 6 (noting that AOL has market incentives to protect its subscribers' personal information).

[99] *See, e.g.*, Charter Comments at 8 (noting that recent studies demonstrate that nearly 60% of consumers either terminate service or consider switching service providers when a company fails to protect personally identifiable information); NASUCA Comments ar 26 (arguing that rhe Commission should *not rely* alone on *the* "good business sense" of carriers to notify their customers of a security breach).

[100] As EPIC states by way of example, such notice will "allow individuals to take actions to avoid stalking or domestic violence, . . . and also allow individuals to pursue private claims against the pretexter or person employing the pretexter." EPIC *et al.* Comments at 15.

CPNI is disclosed pursuant to the "except as required by law" exception contained in section 222(c)(1), such disclosure does not trigger the carrier's obligation to notify a customer of any "unauthorized" access to CPNI.[101] We further clarify that nothing in today's 01-der is intended to mandate customer notice when providers of covered services ai-e permitted by law to disclose customers' personal information. such as to "protect the rights or propeny of the carrier. or to protect users of those services and other carriers from fraudulent. abusive. or unlawful use of. or subscription to. such services.."'"' Further. we do not intend to supersede any statute. regulation. order. or interpretation in any state. except to the extent that such statute. regulation. order. or interpretation is inconsistent with the provisions of this section. and then only to the extent of the inconsistency.

32. *Content of Customer Notice.* We decline to specify the precise content of th notice that must he provided to customers in the event of a security breach of CPNI. The notice req. ement we adopt in this proceeding is general. and we recognize that numerous types of circumstances – including situations other than pretexting – could result in the unauthorized disclosure of a customer's CPNl to a third party. Thus. we leave carriers the discretion to tailor the language and method of notification to the circumstances.[103] Finally. we expect carriers to cooperate fully in any law enforcement investigation of such unauthorized release of CPNl or attempted unauthorized access to an account consistent with statutory and Commission requirements.

C. Additional Protection Measures

33. *Guarding Against Pretexting.* We agree with commenters that techniques for fraud vary and tend to become more sophisticated over time. and that carriers need leeway to engage emerging threats.'"[104] We therefore clarify that carriers are free to bolster their security measures through additional measures to meet their section 222 obligations to protect the pi-ivacy of CPNI.[105] We also codify the existing statutory requirement contained in section 222 of the Act that carriers take reasonable measures to discover and protect against activity that is indicative of pretexting.[106] As we discuss below. adoption of the rules in this Order does not relieve carriers of their fundamental duty to remain vigilant in their protection of CPNI, nor does it necessarily insulate them from enforcement action for unauthorized disclosure of CPNI.

34. Although we expect that carriers will use forms of *self-monitoring* to comply with this obligation, at this time we allow carriers to determine what specific measures will best enable them to

[101] See DOJ/DHS Comments at 14. In particular. a carrier is not required to notify the subject of a lawful investigation that law enforcement has sought or obtained access to the subject's telephone records. which could jeopardize the investigation. As the Department of Justice explains, Congress already has established a structure for customer notification of law enforcement access to customer records for providers of certain services. and by our action today we do not disturb the balance Congress has struck on this issue for such providers. See *id.* at 15-16 (citing 18 U.S.C. §§ 2701 *et seq.*).

[102] 47 U.S.C. § 222(d); see *also* I8 U.S.C. § 2702.

[103] NASUCA urges carriers to provide individualized notice to customers in the event of a security breach because notice in a bill may not be read by the customer. See NASUCA Comments at 7-8.

[104] See. *e.g.*, CTIA Comments at 6 (explaining that carriers must respond to a constantly evolving threat from pretexters who become more knowledgeable with every call to a carrier's customer service representatives).

[105] For example. several carriers already voluntarily refuse to divulge call detail information directly over the telephone even with password protection. *See. e.g.*, Letter from Brian F. Fonter. Vice President. Federal Relations. Cingular Wireless LLC. to Marlene H. Dortch. Secretary. FCC. CC Docket No. 96-115 (filed Sept. 29. 2006); Letter from William F. Maher. Jr.. Counsel for T-Mobile LISA. Inc.. to Marlene H. Dortch. Secretary. FCC. CC Docket No. 96-115 at 2 (filed Dec. 4. 20061.

[106] Section 222(a) of the Act imposes a generally duty on carriers to "protect the confidentiality of proprietary information of. and relating to . . . customers." 47 U.S.C. § 222(a).

ensure compliance with this requirement.[107] By codifying a general requirement to take reasonable measures to discover and protect against activity that is indicative of pretexting. we permit carriers to weigh the benefits and burdens of particular methods of possibly detecting pretexting. This approach will allow carriers to improve the security of CPNl in the most efficient manner possible:"" and better enable small businesses to comply with our rules.

35. We stress our expectation that can-iei-s will take affirmative measures to discover and protect against activity that is indicative of prelexting beyond what is required hy the Commission's current rules.[109] and remind carriers that the Act imposes on them the duty of instituting effective measures to protect the privacy of CPNI."" Moreover, as discussed in the Enforcement Section, *infra*,[111] by requiring carriers to demonstrate that they have taken adequate measures to guard against pretexting. we give carriers adequate incentive to uncover situations where they have released CPNl to a third party without authorization. We anticipate that a carrier that practices willful blindness with regard to pretexting would not be able to demonstrate that it has taken sufficient measures to guard against pretexting. Although, we do not adopt specific rules in this Order that fully encompass this affirmative duty, we seek comment in our Further Notice on whether the Commission should require carriers to utilize audit trails and comply with certain data retention requirements.[112]

36. *Network Security.* In response to EPIC's encryption proposal. we make clear that carriers' existing statutory obligations to protect their customers' CPNl include a requirement that carriers take reasonable steps. which may include encryption. to protect their CPNl databases from hackers and other unauthorized attempts by third parties to access CPNI."' Although several carriers report that they have looked for. but not found. attempts by outsiders lo penetrate their CPNl databases directly,[114] commenters also report that pretexters' methods for gaining access to data evolve over time.[115] As carriers take stronger measures to safeguard CPNl. data brokers may respond by escalating their techniques to access CPNI. such as through hacking. Therefore. although we decline at this time specifically to require carriers to encrypt their CPNl databases. we interpret section *222* as requiring carriers lo protect CPNl when it is stored in a carrier's databases."'

---

[107] See. *e.g.*, Missouri PSC Comments at 3 (pointing out that audit trails are useful when tracking and prosecuting entities that obtain CPNl dishonestly or inappropriately): NCTA Comments at 4 (arguing that while audit trails do not deter pretexting. they can help carriers identify and investigate security breaches after they have occurred).

[108] Moreover. as numerous commenters observe. publishing criteria for identifying suspect calls or calling patterns or online attempts at access would aid pretexters more than it would enhance security. See, *e.g.*, CTIA Comments at 3: T-Mobile Comments at 4: US Telecom Comments at 3-4 (arguingthat overly-specific rules risk giving pretexters a "roadmap").

[109] This expectation is reasonable given that the problem of pretexting emerged notwithstanding the Commission's current rules.

[110] 47 U.S.C. § 222(c); 47 C.F.R. § 64.2009.

[111] *See infra* Section IV.I.

[112] See Further Notice at paras. 69-70

[113] See EPIC Petition at 11

[114] *See. e.g.*. AT&T Comments at 15-16: Cingular Comments at 13: Verizon Wireless Comments at 11.

[115] *See. e.g.*. Centennial Reply at 7.

[116] Commenters report that the expense of encryption would be substantial. and would be of limited value in protecting against pretexting. *See. e.g.*, Verizon Wireless Comments at 11. Some carriers nevertheless may find that encryption currently is a cost-effective way to increase the security of CPNl. *See. e.g.*, Alltel Comments at 6 (noting that Alltel is encrypting some data stores to stop potential hackers). In addition. if carriers begin to

(continued....)

D. Joint Venture and Independent Contractor Use of CPNI

37. We modify our rules to require telecommunications carriers to obtain opt-in consent from a customer before disclosing that customer's CPNI to a carrier's joint venture pnnner or independent contractor for the purpose of marketing communications-related services to that customer.[117] While we realize that this is a change in Commission policy. we find that new circumstances force us to reassess our existing regulations. As we have found previously, the Commission has a substantial interest in protecting customer privacy."' Based on this and in light of new privacy concerns. we now find that an opt-in framework for the sharing of CPNI with joint venture partners and independent contractors for the purposes of marketing communications-related services to a customer both directly advances our interest in pi-otecting customer privacy and is narrowly tailored to achieve our goal of privacy protection. Specifically. an opt-in regime will more effectively limit the circulation of a customer's CPNI by maintaining it in a carrier's possession unless a customer provides informed consent for its release. Moreover. we find that an opt-in regime will provide necessary informed customer choice concerning these information sharing relationships with other companies.

38. In the *Notice*. the Commission sought comment on whether the existing opt-out regime is sufficiently pi-otective of the privacy of CPNI when CPNI is disclosed to telecommunications carriers' joint venture partners and independent contractors. and whether the Commission should instead adopt an opt-in policy for this type of CPNI sharing.[119] The cui-rent opt-out regime allows for carriers to share CPNI with joint venture partners and independent conti-actors for the purposes of marketing communications-related services after providing only a notice to a customer.[120] The burden is then placed on the customer to opt-out of such sharing arrangements. If the customer does not respond. a carrier's sharing of customer information with these entities is allowed.

39. We find that there is a substantial need lo limit the sharing of CPNI with others outside a customer's carrier to protect a customer's privacy. The black market for CPNI has grown exponentially with an increased market value placed on obtaining this data. and there is concrete evidence that the dissemination of this private information does inflict specific and significant harm on individuals, including harassment and the use of the data to assume a customer's identity.'" The reality of this private information being disseminated is well-documented and has already resulted in irrevocable damage to customers.[122] While there are safeguards in our current rules for sharing CPNI with joint venture partners

(...continued from previous page)
experience increased attempts to obtain CPNI through hacking or similar measures. we would expect all carriers to revisit whether encryption of CPNI databases would satisfy their obligation to take reasonable steps to protecl CPNI databases from unauthorized third-party access.

[117] We do not believe that this minor change to our rules will have a major effect on carriers because many carriers already do not disclose CPNI to third parties. ***See. e.g.***, CTIA Comments at 12 (noting that most wireless carriers do not disclose CPNI to third parties or use it outside of a total service approach): US Cellular Reply at 2 (stating that it does not share CPNI other than in accordance with the total service approach). Additionally. we note that this opt-in regime does not in any way affect a carrier's permitted use of CPNI enumerated in section 222(d). 41 U.S.C. § 222(d).

[118] ***See Third Report arid Order***. 17 FCC Rcd at 14875-75, para. 33: ***see*** also. ***e.g.***. Joint Commenters Comments at 16 (stating that they do not dispute that the Commission has a substantial interest in protecting privacy).

[119] ***SPP Notice.*** 21 FCC Rcd at 1788. para. 12

[120] *See* 47 C.F.R. § 64.2007(b)(1): *see also, e.g.*. NASUCA Comments at 9 (arguing that with an opt-out policy "there is no assurance that an) implied consent would he truly informed").

[121] *See, e.g., supra* para. 12 and accompanying notes: *Telephone Records and Privacy Protection Act of 2006*. H.R. 4709, 109th Cong. i2d Sess. 2006).

[122] *See, e.g., supra* para. 12 and accompanying notes

and independent contractors.[123] We hrlieve that these safeguards do not adequately protect a customer's CPNI in today's environment. Specifically. we find that once the CPNl is shared with a joint venture partner or independent contractor. the can-ier no longer has control over it and thus the potential for loss of this data is heightened."[124] We find that a carrier's section 222 duty to protect CPNl extends to situations where a carrier shares CPNl with its joint venture partners and independent contractors. However. because a carrier is no longer in a position to personally protect the CPNl once it is shared – and section 222's duties may not extend to joint venture partners or independent contractors themselves in all cases – we find that this sharing of data. while still permitted. warrants a requirement of express prior customer authorization."[125]

40. We agree with commenters that argue that the current opt-out notices allowing carriers to share information with joint venture partners and independent contractors ai-e often vague and not comprehensible to an average customer.[126] Further. we find that many consumel- studies on opt-out regimes also reflect this consumer confusion."[127] We do not believe that simply modifying our existing opt-out notice requirements will alleviate these concerns because opt-out notices do not involve a customer actually authorizing the sharing of CPNl in the first instance. but rather leave it to the carrier to decide whether to share it after sending a notice to a customer. which a customer may or may not have read.[128] While many customers accept and understand that carriers will share their information with affiliates and agents – as provided in our existing opt-out rules – there is less customer willingness for their information to he shared without their express authorization with others outside the carrier-customer relationship.[129]

41. We disagree with commenters that assert that an opt-in approach will not serve to remedy the concerns raised in this pi-ocrrding."[130] The Attorneys General note that since February 2005, security breaches have resulted in the personal information of over 54 million Americans being compromised."[131] With the growing interest in obtaining customer CPNl and the resulting increase in the number of security breaches. carriers must be more vigilant in protecting a customer's CPNl from unauthorized disclosure."[132]

---

[123] 47 C.F.R. § 64.2007(b)(2).

[124] See. *e.g.*, MoPSC Comments at 4 (asserting that there is a lack of control over third-party recipients of CPNI)

[125] *See* 47 U.S.C. § 222.

[126] *See, e.g.*, EPIC *et al.* Comments at 7: MoPSC Comments at 5.

[127] See Attorneys General Comments at 6 (noting studies surrounding Gramm-Leach-Bliley Act. including a study by Harris Interactive. Inc.); MoPSC Comments at 5 (noting that during the state's rulemaking on CPNl protections. it found that the concept of opt-out was not understandable to the average consumer).

[128] See. *e.g.*, Attorneys General Comments at 6 (arguing that most customers are unlikely to read opt-out notices and therefore not know that they are giving affirmative consent to share their information): NASUCA Comments at 9 (believing that customers might not read CPNl notices and thus they are unaware that they might need to take affirmative action to prevent the sharing of their personal information).

[129] See. *e.g.*, EPIC *et al.* Comments at 9-10 (pointing to a series of studies finding that consumers support opt-in privacy policies generally): NASUCA Comments at 9 (arguing that opl-in approval better protects a customer's privacy and gives the customer more control over the sharing of their personal information): Privacy Rights Comments at 4 (arguing that only opt-in consent provides adequate privacy protection).

[130] *See, e.g.*, Alltel Comments at 3-4: AT&T Comments at 17- 19: Cingular Comments at 14: CTIA Comments at 12: Joint Commencers Comments at 12: TWTC Comments at 16: Verizon Comments at 22-26: Verizon Wireless Comments at 10: DMA Reply at 1-2.

[131] Attorneys General Comments at 7-9 (noting that there are over 152 major security breaches reported since February 2005 resulting in the loss of information to at least 54 million Americans).

[132] *See* 47 U.S.C. § 222; *see also supra* note 121

It stands to reason that placing customers' personal data in the hands of companies outside the carrier-customer relationship places customers ai increased risk. not only of inappropriate handling of the information. hut also of innocent mishandling or loss of control over it. Further. we find that an opt-in regime will clarify carriers' information sharing practices because it will force carriers to provide clear and comprehensible notices to their customers in order to gain their express authorization io engage in such activity.

42. We also disagree with commenters that argue that the current opt-out approach is sufficient. and that in the event of a breach. a carrier can terminate its relationship with the joint venture panner or independent contractor. or that the Commission can simply deal with the situation through an enforcement proceeding.[133] We find that in the event of a hi-each of CPNl security. the damage is already inflicted upon the customer. We also find that the carrier cannot simply rectify the situation by terminating its agreement nor can the Commission completely alleviate a customer's concerns about the privacy invasion through an enforcement proceeding.[134]

43. This minor modification of our rules seeks to narrow the number of avenues available for an unauthorized disclosure of CPNl without eliminating a carrier's ability to share CPNl with its joint venture panners and independent contractors under certain circumstances. We disagree that an opt-in regime's costs outweigh the benefits to customers.[135] While we appreciate commenter concern that carriers may need to engage in broader marketing campaigns for their sei-vices as a result of an opt-in regime. we believe that this cost is outweighed by the carriers' duty to protect their customers' private information. and more importantly. customers' interest in maintaining control over their private information.[136] Thus. we believe that an opt-in regime is the least restrictive means to ensure that a customer has control over its private information and is not subjected to permanent harm as a result of a carrier's disclosure of CPNl to one of its joint venture partners or independent contractors.[137]

44. We disagree with commenters who assert that an opt-in regime for disclosures to joint venture panners and independent contractors fails the *Central Hudson* test[138] for the regulation of commercial speech.[139] We recognize that more than seven years ago, in *U.S. West, Inc. v. FCC*, the United States Coun of Appeals for the Tenth Circuit held that the Commission had failed, based on the record in that proceeding, to satisfy its burden of showing that an opt-in rule passed the *Central* Hudson test.[140] That decision, however, was based on a different record than the one compiled here and, in

---

[133] See. *e.g.*, Cingular Comments at 14: COMPTEL Comments at 4.

[134] We note that while our enforcement actions may act as a deterrent to a carrier's unauthorized use of CPNI. they cannot undo the harm to a customer after a breach.

[135] *See. e.g.*, BellSouth Comments at 26-27.

[136] *Compare* Verizon Comments at 26 *with* 41 U.S.C. § 222.

[137] We note that this minor modification to our rules does not affect the opt-out regime for intra-company use o f CPNl beyond the total service approach. or the disclosure of CPNl to a carrier's agents or affiliates that provide communications-related services.

[138] *Central Hudson.* 447 U.S. at 564-65. The *Central Hudson* test provides that if the commercial speech concerns lawful activity and is not misleading. the government may restrict the speech only if it (1) "has a substantial state interest in regulating the speech. (2) the regulation directly and materially advances that interest. and (3) the regulation is no more extensive than necessary to serve the interest." *Central Hudson*. 441 U.S. at 564-65.

[139] *See. e.g.*. BellSouth Comments at 27; Joint Commenters Comments at 14-16; TWTC Comments at 16-17; Verizon Comments at 23-25; Verizon Wireless Comments at 11-12; BellSouth Reply at 3-9; Charter Reply at 3-14; Verizon Reply at 2-8.

[140] *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999)

particular. on two premises that are no longer valid. First. the Tenth Circuit concluded that there was no rvidence showing harm to privacy interests from unauthorized disclosure of CPNI. "While protecting against disclosure of sensitive and potentially embarrassing personal information may be important in the abstract. we have no indication of how it may occur in reality with respect to CPNI. Indeed. we do not even have indication that the disclosui-e might actually occur."[141] The record in this proceeding, by contrast. is replete with specific examples of unauthorized disclosure of CPNl and the adverse effects of such disclosures on customers.[142] Indeed. in the Telephone Records and Privacy Protection Act of 2006. Congress recently found that unauthorized disclosure of telephone records is a problem that "not only assaults individual privacy but. in some instances. may further acts of domestic violence or stalking. compromise the personal safety of law enforcement officers. their families. victims of crime. witnesses. or confidential informants. and undermine the integrity of law enforcement investigations."[143] Second. the Tenth Circuit in *U.S. West* concluded that the record "d|id] not adequately show that an opt-out strategy would not sufficiently protect customer privacy."[144] In this proceeding. however, substantial evidence shows that the current opt-out rules do not adequately protect customer privacy because most customers either do not read or do not understand carriers' opt-out notices.[145] For example, the National Association of Attorneys General cites to "studies [that] serve as confirmation of what common sense tells us: that in this harried country of multitaskers. most consumers are unlikely to read extra notices that arrived in today's or last week's mail and thus. will not understand that failure to act will he treated as an affirmative consent to share his or her information."[146]

45. We find. based on the record in this proceeding. that requiring carriers to obtain opt-in consent from customers before sharing CPNI with joint venrure partners and independent contractors for marketing purposes satisfies the *Central Hudson* test. Specifically. we find that: (1) unauthorized disclosure of CPNl is a serious and growing problem: (2) the government has a substantial interest in preventing unauthorized disclosure of CPNl because such disclosui-e can have significant adverse consequences for pi-ivacy and safety;[147] (3) the more independent entities that possess CPNI. the greater the danger of unauthorized disclosui-e: (4) an opt-in regime directly and materially advances privacy and safety interests by giving customers direct control over the distribution of their private information outside the carrier-customer relationship; and (5) an opt-in regime is not more extensive than necessary to protect privacy and safety interests because opt-out rules, the alternative cited by the Tenth Circuit in *U.S. West, Inc. v. FCC*, do not adequately secure customers' consent for carriers to share CPNl with unaffiliated entities. In short, given the undisputed evidence demonstrating that unauthorized disclosures of CPNl constitute a serious and prevalent problem in the United States today, we believe that carriers should be required to obtain a customer's explicit consent before sending such sensitive information outside of the company for marketing purposes. In light of the serious damage that unauthorized CPNl disclosures can cause, it is important that individual consumers determine if they want to bear the increased risk associated with sharing CPNl with independent contractors and joint venture partners, and the only way to ensure that a consumer is willingly bearing that risk is to require opt-in consent. In this vein, we note that most United States privacy laws, such as the Family Educational Rights and Privacy Act, Cable Communications Policy Act, Electronic Communications Privacy Act, Video Privacy

[141] *Id.* at 1237.

[142] *See supra* para. 10 and accompanying notes: *see also. e.g.*. Attorneys General Comments at 1-4: NASUCA Reply at 12.

[143] Telephone Records and Privacy Protection Act of 2006. Pub. L. No. 109-476. 120 Stat. 3568. § 2(5) (2007)

[144] *U.S. West. Inc. v. FCC*, 182 F.3d at 1239

[145] *See supra* para. 36 & nn.124-25

[146] Attorneys General Comments at 6

[147] *See also U.S. West. Inc. ,. FCC.* IS' F.3d at 1236.

Pi-oteciion Act. Driver's *Privacy Protection Act*. and Children's Online Privacy Protection Act. do not employ an opt-out approach hut rather require an individual's explicit consent before private information is disclosed or employed for secondary purposes.[148]

46. We disagi-ee with commenters who contend that requiring carriers to obtain opt-in consent from customers before sharing CPNl is unnecessary because. they claim. there is no evidence that data brokers have obtained CPNl from carriers' joint venture panners and independent contractors.[149] While it is ti-ue that the record does not include specific examples of unauthorized disclosure of CPNI by a joint venture panner or independent contractor. that does not mean unauthorized disclosure has not occurred or will not occur in the future. We see no reason why joint venture partners and independent contractors would be immune from this widespread problem. While carriers ai-gue that pretexters do not focus their efforts on independent contractors and joint venture partners. we disagree with commenters who sug: .st that the governmental interests at slake in this proceeding are limited to the prevention of pretexting.[150] The rules we are adopting are designed to curtail *all* forms of unauthorized disclosure of CPNI. not just pretexting. Unauthorized disclosure of CPNl by any method invades the privacy of unsuspecting consumers and increases the risk of identity theft. harassment. stalking, and other threats to personal safety.[151] In this proceeding. commenters have identified at least two other *common forms* of unauthorized disclosure of CPNI: computer intrusion and disclosure by insiders.[152] Indeed. evidence in the record suggests that 50-70% of cases of identity theft arise from wrongful conduct by insiders.[153] The record further demonstrates that *information* security breaches are on the rise in this country. and it is axiomatic that the more companies that have access to CPNI. the greater the risk of unauthorized disclosure through disclosure by insiders or computer intrusion.[154] Thus. by sharing CPNl with joint venture panners and *independent contractors*. it is clear that carriers increase the odds of wrongful disclosure of this sensitive information. and before the chances of unauthorized disclosure are increased. a customer's explicit consent should be required. In any event. returning to the issue of pretexting, we also reject the ai-gumen! that pretexters do not attempt to obtain CPNl from independent contractors and joint

[148] EPIC *et al*. Comments at 9. Moreover. Verizon contends that consumers have found "the mechanics of the opt-in regime . . . confusing" and have been reluctant to use opt-in. that is based on its experiences following the Commission's 2001 *Clarification Order*. *See* Verizon Jan. 29 Ex *Parte* Letter. Verses Decl. at para. 16. We note. however. that in the intervening years the use of opt-in approval methods appear to have become increasingly common. such as in the *mobile* wireless *context*. and thus we do not find Verizon's past experiences persuasive. See, *e.g.*, The *Mobile Revolution Will* Be *Advertised*, Wireless Business Forecast. 2006 WLNR 491 1016 (Mar. 23. 2006) (discussing the use of opt-in approval processes in mobile wireless marketing): Betsy Spethmann, *Next-Tech.*, Promo, *2005* WLNR 10551271 (July 1.2005) (discussing the use of an opt-in approval process by Verizon Wireless).

[149] See Verizon Jan. 29.2007 *Ex Parte* Letter at 3: Lerter from William Maher. Ir.. Counsel for T-Mobile USA. Inc. to Marlene Dortch. Secretary. FCC. CC Docket No. 96-115 at *3* (filed Jan. 25,2007) (T-Mobile Jan. 25 *Ex Parte* Letter): Letter from Kathryn Marie Krause. Qwest. to Marlene Dortch, Secretary. FCC. CC Docket No. 96-115 at *3* (filed Jan. 18.2007) (Qwest Jan. 18. 2007 *Ex Parte* Letter).

[150] *See* Verizon Jan. 29.2007 *Ex Parte* Letter at 20-22; Letter from Kent Nakamura. Vice President and Chief Privacy Officer. Sprint Nextel. to Marlene Dortch. Secretary. FCC. CC Docket No. 96-115 at 1 (filed Jan. 26.2007) Sprint Nextel Jan. 26.2007 *Ex Parte* Letter): Letter from James Jenkins. Vice President. United States Cellular Corp.. to Marlene Dortch. Secretary. FCC. CC Docket No. 96-115 at 1 (filed Feb. 5.2007): T-Mobile Jan. 25.2007 *Ex Parte* Letter at 3: Qwest Jan. 18. 2007 *Ex Parte* Lerter at 3: Lerter from *Anisa Latif*. AT&T. to Marlene Dortch. Secretary. FCC. CC Docket No. 96-115 at 1 (filed Jan. 17.2007).

[151] *See* Telephone Records and Privacy Protection Act of 2006, § 2: NASUCA Reply at 12.

[152] *See* Attorneys General Comments at 3: EPIC Comments at 5: NASUCA Reply at 11

[153] EPIC Comments at 6

[154] *See, e.g.*, EPIC Comments at 6: NASUCA Reply at 15